Office of the Information and
Privacy Commissioner of Alberta

PERSONAL INFORMATION PROTECTION ACT
Breach Notification Decision

Organization providing notice under section 34.1 of PIPA	Industrial Alliance Insurance and Financial Services Inc. (Organization)
Decision number (file number)	P2019-ND-161 (File #013313)
Date notice received by OIPC	May 24, 2019
Date Organization last provided information	May 24, 2019
Date of decision	November 19, 2019
Summary of decision	There is a real risk of significant harm to the individuals affected by this incident. The Organization is required to notify the individual whose personal information was collected in Alberta pursuant to section 37.1 of the *Personal Information Protection Act* (PIPA).
JURISDICTION	
Section 1(1)(i) of PIPA "organization"	The Organization is an "organization" as defined in section 1(1)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident may have involved all or some of the following information: • first and last name, • Social Insurance Number, • banking information, • health information, • date of birth, and • address. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent the personal information was collected in Alberta, PIPA applies.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• An employee of an agency of the Organization was the victim of a phishing incident in the fall of 2018. All the victims of this first incident resided in Quebec.

	• After resetting his password, the employee inadvertently used his old password that had been the subject of the phishing incident. The hacker was again able to take control of the mailbox and had the opportunity to access all the emails in the employee's mailbox and the personal information in the emails. • The hacker took control of the email box and sent phishing emails to contacts obtained from the email box. • The incident was discovered by the employee on February 27, 2019.
Affected individuals	The incident affected 2,170 individuals, including one whose information was collected in Alberta.
Steps taken to reduce risk of harm to individuals	• Took steps to regain control of the compromised email box and ended the unauthorized access. • Launched training for the sales force on May 14, 2019. • Undertaking phishing tests to confirm the understanding of employees and the sales force. • More robust security measures have been put in place for the employee concerned. • The corporate rules for creating passwords are being revised. • A credit monitoring service for a period of 12 months was offered to all the notified customers.
Steps taken to notify individuals of the incident	Affected individuals were notified by letter on May 24, 2019.
REAL RISK OF SIGNIFICANT HARM ANALYSIS	
Harm Some damage or detriment or injury that could be caused to affected individuals as a result of the incident. The harm must also be "significant." It must be important, meaningful, and with non-trivial consequences or effects.	The Organization reported … *Considering the fact that our investigation concluded that the person who took control of the email box primarily intended to use it to send other malicious e-mails from the e-mail inbox and not to use the personal information contained in the email box, we do not believe that there is* ***a*** *significant risk of real harm. There is however a small possibility of identity theft or fraud, which could lead to economic loss.* *Also, given that some customers were notified of a breach of confidentiality of their personal information a second time, these customers may suffer additional stress.* In my view, a reasonable person would consider the identity, financial and health information at issue could be used to cause the harms of identity theft and fraud, as well as hurt, humiliation and embarrassment. Email addresses could be used for phishing

	purposes, increasing vulnerability to identity theft and fraud. These are all significant harms.
Real Risk The likelihood that the significant harm will result must be more than mere speculation or conjecture. There must be a cause and effect relationship between the incident and the possible harm.	The Organization reported that the likelihood of significant harm resulting was "Low, considering the fact that the person who took control of the e-mail box primarily intended to use it to send other malicious e-mails from the e-mail box and not to use the personal information in the contents of the box...". The likelihood of harm resulting from this incident is increased as the breach was the result of malicious intent (phishing) by an unknown third party and the personal information was used to send additional phishing emails. The Organization can only speculate as to the intent of the hacker.

DECISION UNDER SECTION 37.1(1) OF PIPA

Based on the information provided by the Organization and given the circumstances of the incident, I have decided that there is a real risk of significant harm to the affected individuals.

A reasonable person would consider the identity, financial and health information at issue could be used to cause the harms of identity theft and fraud, as well as hurt, humiliation and embarrassment. Email addresses could be used for phishing purposes, increasing vulnerability to identity theft and fraud. These are all significant harms.

The likelihood of harm resulting from this incident is increased as the breach was the result of malicious intent (phishing) by an unknown third party and the personal information was used to send additional phishing emails. The Organization can only speculate as to the intent of the hacker.

I require the Organization to notify the affected individual in Alberta in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation).

I understand the affected individual was notified by letter on May 24, 2019. The Organization is not required to notify the affected individual again.

Jill Clayton
Information and Privacy Commissioner